DIT

Privacy Threshold Analysis (PTA)

Submission and Renewal Process

August 2018

Table of Contents

I.   Introduction

The Privacy Threshold Analysis (PTA) is a required document that serves as the official determination by the Enterprise Security and Risk Management Office (ESRMO) as to whether a State program or system has privacy implications, and if additional privacy compliance documentation is required. The PTA is built into the ESRMO processes for technology investments and security. PTAs expire and must be reviewed and re-certified every year or when a change to the environment and security posture occurs.

The PTA:

- Identifies programs and systems that are privacy-sensitive, i.e. Restricted or Highly Restricted data per N.C.G.S. § 132.1-6(c)

- Demonstrates the inclusion of privacy considerations during the review of a program or system

- Provides a record of the program or system and its privacy requirements to the ESRMO

- Demonstrates compliance with privacy laws and regulations

Generally, a PTA is required before a program or system containing Restricted or Highly Restricted data becomes operational. N.C.G.S. § 132-1.10 establishes the following reasons for conducting a privacy analysis:

- Government should collect the information only for legitimate purposes or when required by law

- Social security numbers collected by an agency must be relevant to the purpose for which collected and shall not be collected until and unless the need for social security numbers has been clearly documented.

- Restrict the use of social security numbers for any purpose other than the purpose stated

II.   Purpose

DIT is establishing this PTA process to (a) create and formalize the existing set of PTAs into a baseline repository and (b) make use of the new electronic submission process for all new PTAs so that the repository can be maintained going forward. This document outlines the following steps State agencies need to take to provide PTAs:

a. Capture the types of data that are used for **all** agency applications.

b. Consolidate the State's current inventory of PTA forms into one repository. This will aid both DIT and other agencies in knowing what data has been reported and what PTAs have been filed.

c. Submit all future PTAs through the new electronic PTA process.
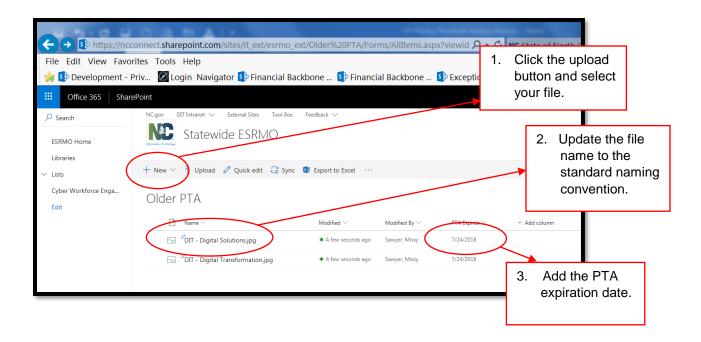
III.   Scope

This process document applies to all State agencies, departments and other entities not specifically excluded from Article 15 of N.C. General Statute Chapter 143B.

IV.   Roles and Responsibilities

The Agency's Data Owner or designee is responsible for completing the PTA in cooperation with the Agency's privacy/security officer. Once the PTA is complete, the Agency privacy/security officer will submit the PTA to the ESRMO for review.

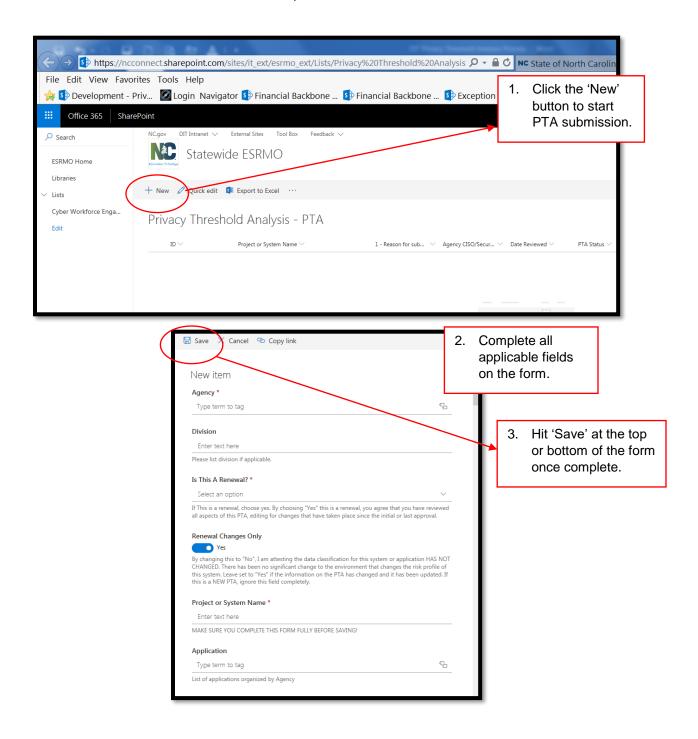## V. Gathering the Initial PTA Inventory of Existing Applications

1. The ESRMO will make available to the Agencies all PTAs that are on file and were submitted through the statewide exception process.

2. If the Agency identifies a PTA that is not present in the SharePoint folder, the Agency will upload previously submitted PTAs to the "Older PTA" folder in SharePoint.

   a. Use the current APM list as a reference and the list of PTAs already uploaded.

   b. Please use this standard naming convention:

      i. 'Agency acronym' – 'Application name' – 'Date Agency signed'

      ii. Use the application name from the provided APM list

   c. Fill out the expiration field

      i. The expiration date of a PTA is a year after the Agency Security Liaison approves and submits the PTA to DIT.

VI.   New PTA Submission Process

Agencies will utilize the new electronic PTA form for all new submissions.

a. Complete all applicable PTA fields for your system.

b. Project or System name should either be your application name from the APM tool or your project name from Touchdown.
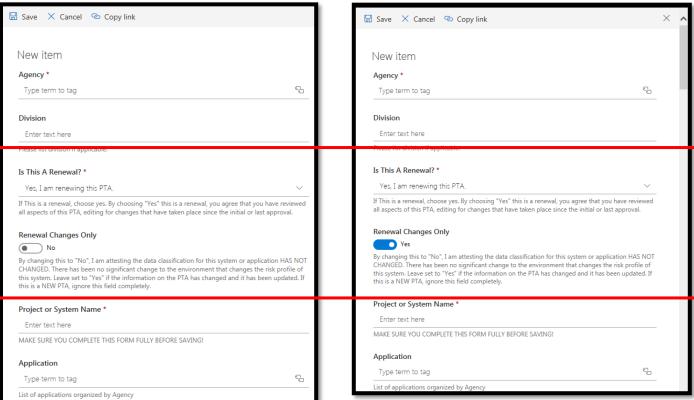
c. Press the "Save" button once complete.

VII. Annual PTA Update Process

1. Email will be sent to the submitter and to the ESRMO 60 days (1st notice) and 30 days (2nd notice) prior to the PTA expiration date* informing them that their PTA is expiring.

2. Email will be sent to both the submitter and ESRMO team if the PTA hits it's expiration date.

3. Submitter will go into their PTA to review for any required changes.

   a. If changes are NOT required:
      - Submitter will answer "Yes, I am renewing this PTA"
      - Change the "Renewal Changes ONLY" slide button to "No"
      - Hit "Save" at the bottom of the form

   b. If changes are required:
      - Submitter will answer "Yes, I am renewing this PTA"
      - Change the "Renewal Changes ONLY" slide button to "Yes"
      - Make all applicable changes throughout the form
      - Hit "Save" at the bottom of the form

Changes NOT required   Changes required

* PTA expiration is 365 days after submission

VIII. <u>Data Glossary</u>

Health Insurance Portability and Accountability Act (HIPAA)
- Medical and substance abuse

Personally Identifiable Information (PII)
- Public (Non-Sensitive):
    - Address information, such as street address or email address
    - Mail lists
- Non-Public (Sensitive):
    - SSN
    - Driver's License or State Identification Number
    - Passport Number
    - Alien Registration Number
    - Financial Account Number
    - Medical Information
    - Mother maiden name
    - Biometric data

Payment Card Industry (PCI)
- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Service Code
- Full track data (magnetic-stripe data or equivalent on an chip)
- CAV2/CVC2/CVV2/CID
- PINs/PIN blocks
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)

Criminal Justice Information (CJI)
- Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

- Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

- Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

- Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
- Case/Incident History—information about the history of criminal inc

Federal Tax Information (FTI)

- Information, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense

- Information extracted from a return, including names of dependents or the location of business

- The taxpayer's name, address, and identification number

- Information collected by the IRS about any person's tax affairs, even if identifiers, such as name, address, and identification number are deleted

- Status of whether a return was filed, under examination, or subject to other investigation or processing, including collection activities

- Information contained on transcripts of accounts

Family Educational Rights and Privacy Act (FERPA)
- Directory information such as a:
  - Student's name
  - Student address
  - Student telephone number
  - Date and place of birth
  - Honors and awards
  - Dates of attendance

Other Categories of sensitive data types:

- These are data types that have been defined by State law as not publicly releasable without first being redacted:
  - Security assessment reports
  - Network/System vulnerabilities